IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use, said computer program comprising:

(i) user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

(ii) banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;

wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed.

2. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data is encrypted with a private key.

3. (Cancelled)

4. (Previously Presented) A computer program product as claimed in claim 1, wherein said banned program identifying data controls said anti computer virus logic to

identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

5. (Previously Presented) A computer program product as claimed in claim 4, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

6. (Original) A computer program product as claimed in claim 1, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

7. (Currently Amended) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising a non-virus computer program, said computer program comprising:

[[(i)]] anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;

wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use;

wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

8. – 10. (Cancelled)

11. (Previously Presented) A computer program product as claimed in claim 7, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

12. (Currently Amended) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising a non-virus computer program, said computer program comprising:

anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;~~as claimed in claim 7,~~

wherein said anti computer virus logic respon[[ses]]ds to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

13. (Original) A computer program product as claimed in claim 7, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

14. (Original) A computer program product as claimed in claim 7, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

15. (Currently Amended) A method of generating banned program identifying data indicative of at least one computer program to be banned from use, said method comprising the steps of:

[[(i)]] user specifying at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

[[(ii)]] generating banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;

wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed.

16. (Original) A method as claimed in claim 15, wherein said banned program identifying data is encrypted with a private key.

17. (Cancelled)

18. (Previously Presented) A method as claimed in claim 15, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

19. (Previously Presented) A method as claimed in claim 18, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said at least one computer program banned from use that share said behavioral characteristics may also be identified.

20. (Original) A method as claimed in claim 15, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

21. (Currently Amended) A method for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said method comprising the step of:

[[(i)]] in response to receiving user generated banned program identifying data for said at least one computer program to be banned from use, operating anti computer virus logic to identify computer programs banned from use for triggering a banned program action;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;

wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use;

wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

22. – 24. (Cancelled)

25. (Previously Presented) A method as claimed in claim 21, wherein when a banned computer program is identified, said at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

26. (Currently Amended) A method for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said method comprising the step of:

in response to receiving user generated banned program identifying data for said at least one computer program to be banned from use, operating anti computer virus logic to identify computer programs banned from use for triggering a banned program action;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;~~as claimed in claim 21,~~

wherein said anti computer virus logic respon[[ses]]ds to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

27. (Original) A method as claimed in claim 21, wherein said anti computer virus logic is executable as a separate instance solely to identify computer programs banned from use.

28. (Original) A method as claimed in claim 21, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

29. (Currently Amended) Apparatus for generating banned program identifying data indicative of at least one computer program to be banned from use, said apparatus comprising:

[[(i)]] a user controlled program specifier operable to specify at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

[[(ii)]] banned program identifying data generator responsive to said user controlled program specifier to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein the anti computer virus logic identifies computer viruses prior to identifying the computer programs banned from use;

wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed.

30. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data is encrypted with a private key.

31. (Cancelled)

32. (Previously Presented) Apparatus as claimed in claim 29, wherein said banned program identifying data controls said anti computer virus logic to identify said computer programs banned from use in a manner substantially the same as if they were one of the computer viruses.

33. (Previously Presented) Apparatus as claimed in claim 32, wherein said banned program identifying data includes heuristic data identifying at least one behavioral characteristic of at least one computer program banned from use such that variants of said

at least one computer program banned from use that share said behavioral characteristics may also be identified.

34. (Original) Apparatus as claimed in claim 29, wherein said banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

35. (Currently Amended) Apparatus for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said apparatus comprising:

[[(i)]] an anti computer virus system responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus system identifies computer viruses prior to identifying the computer programs banned from use;

wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use;

wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

36.- 38. (Cancelled)

39. (Previously Presented) Apparatus as claimed in claim 35, wherein when a banned computer program is identified, at least one banned program action is triggered, said banned program action comprising at least one of:

(i) issuing an alert message indicating identification of a banned computer program;

(ii) denying access to said banned computer program;

(iii) encrypting said banned computer program; and

(iv) deleting said banned computer program.

40. (Currently Amended) Apparatus for banning from use at least one computer program, said at least one computer program comprising a non-virus computer program, said apparatus comprising:

an anti computer virus system responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein the anti computer virus system identifies computer viruses prior to identifying the computer programs banned from use;~~as claimed in claim 35,~~

wherein said anti computer virus system respon[[ses]]ds to an absence of said user generated banned program identifying data by performing at least one of:

(i) issuing an alert message indicating an absence of said user generated banned program identifying data;

(ii) restoring said user generated banned program identifying data from a remote source;

(iii) disabling a computer upon which said anti computer virus logic is executing.

41. (Original) Apparatus as claimed in claim 35, wherein said anti computer virus system is executable as a separate instance solely to identify computer programs banned from use.

42. (Original) Apparatus as claimed in claim 35, wherein said user generated banned program identifying data comprises data identifying permitted computer programs with all computer programs not matching a permitted computer program being identified as a computer program banned from use.

43. (Previously Presented) A computer program product as claimed in claim 1, wherein the at least one non-virus computer program includes at least one of a game and a data streaming program.

44. (Previously Presented) A computer program product as claimed in claim 1, wherein the at least one non-virus computer program includes games and data streaming programs.

45. (Previously Presented) A computer program product as claimed in claim 1, wherein the anti computer virus logic of a plurality of end users each includes a different selected set of computer programs banned from use.

46. (Cancelled)

47. (New) A computer program product comprising a computer program operable to control a computer to generate banned program identifying data indicative of at least one computer program to be banned from use, said computer program comprising:

user controlled program specifying logic operable to specify said at least one computer program to be banned from use, said at least one computer program comprising a non-virus computer program; and

banned program identifying data generating logic responsive to said user controlled program specifying logic to generate banned program identifying data for said at least one computer program to be banned from use, said banned program identifying data being operable to control anti computer virus logic to identify computer programs banned from use;

wherein an anti-virus scan is performed when a file access request is received, and if said anti-virus scan is not passed, an anti-virus action is triggered and a fail response is returned to an operating system, and if said anti-virus scan is passed, a scan for the computer programs banned from use is performed.

48. (New) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising a non-virus computer program, said computer program comprising:

anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein said banned program identifying data is encrypted with a private key and said anti computer virus logic uses a corresponding public key to decrypt said user generated banned program identifying data prior to use;

wherein said decrypted banned program identifying data is stored within a secured memory region once decrypted.

49. (New) A computer program product comprising a computer program operable to control a computer to ban from use at least one computer program, said at least one computer program comprising a non-virus computer program, said computer program comprising:

anti computer virus logic responsive to user generated banned program identifying data for said at least one computer program to be banned from use to identify computer programs banned from use;

wherein said anti computer virus logic responds to an absence of said user generated banned program identifying data by performing at least one of:

issuing an alert message indicating an absence of said user generated banned program identifying data;

restoring said user generated banned program identifying data from a remote source;

disabling a computer upon which said anti computer virus logic is executing.